IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JOSEPH O. RODGERS, individually and on behalf of all others similarly situated, Plaintiff, v. HOPE COLLEGE, Defendant.	Case No. 23-00109 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMAND**

Plaintiff Joseph O. Rodgers ("Plaintiff") brings this Class Action Complaint ("Complaint"), individually and on behalf of all others similarly situated, against Defendant Hope College ("Hope College" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge.

NATURE OF THE CASE

1. This Class Action Complaint arises out of the recent data breach (the "Data Breach") involving Hope College, which collected and stored certain highly sensitive personally identifiable information of the Plaintiff and the putative Class Members, all of whom have PII on Hope College's servers.

2. According to Hope College, the highly sensitive personally identifiable information that was subject to "unauthorized access" in the Data Breach included: first and last names, date of birth, Social Security numbers, driver's license numbers, and student ID numbers (collectively "PII").

3. Plaintiff brings this Class Action Complaint for Defendant's failure to comply with industry standards to protect its information systems that contain PII and Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been compromised.

4. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the "dark web" black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of credit and identity theft.

5. The Data Breach was a direct result of Hope College's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII. Hope College itself has acknowledged that it first discovered the Data Breach on or around September 27, 2022, but it has only recently begun contacting Class Members starting on December 15, 2022.

6. According to the Office of the Maine Attorney General, who Hope College was required to notify, the Data Breach affected approximately 156,783 individuals.

7. Plaintiff, individually and on behalf of all others similarly situated, brings claims for negligence; negligence *per se*; breach of fiduciary duty; unjust enrichment; breach of implied contract; the Michigan Consumer Protection Act, Mich. Comp. Laws Ann § 445.901, *et. seq.*; and injunctive relief claims.

8. Plaintiff seeks, among other things, damages and injunctive relief requiring Defendant to fully and accurately disclose the PII and other information that has been compromised; to adopt reasonably sufficient security practices and safeguards to protect Plaintiff's

and Class Members' PII from unauthorized disclosures in order to prevent incidents like the Data Breach from reoccurring in the future, and to safeguard the PII that remains in Defendant's custody.

9. Plaintiff further seeks an order requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years, as Plaintiff and Class Members are at risk and will continue to be at an increased risk of identity theft due to the unauthorized disclosure of their PII as a result of Hope College's conduct described herein.

PARTIES

A. Plaintiff

10. Plaintiff Joseph O. Rodgers ("Plaintiff") is a resident of Ingham County, Michigan.

11. On or around December 15, 2022, Plaintiff was notified by Defendant via letter of the Data Breach and of the impact to his PII (the "Notice Letter").

12. Plaintiff's PII was disclosed without his authorization to unknown third parties as a result of Defendant's Data Breach.

13. As a result of Hope College's failure to adequately protect the sensitive information entrusted to it, Plaintiff and Class Members suffered actual damages including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft

– particularly since the compromised information may include Social Security numbers and driver's license numbers.

14. As a result of the Data Breach, Plaintiff has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

B. Defendant

15. Defendant Hope College is a private Christian liberal arts college with its principal place of business at 141 E. 12th Street, Holland, Michigan 49423.

16. Hope College was entrusted with and in possession of Plaintiff's PII.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class Members who are citizens of states other than Defendant's state of citizenship.

18. This Court has personal jurisdiction over Hope College because it is authorized to and does conduct substantial business in this District and is a citizen of this District by virtue of its principal place of business being located in this District.

19. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in Holland, Michigan, which is in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

20. In Hope College's December 15, 2022 Notice Letter to Plaintiff and Class Members, as well as in a "Notice of Data Security Incident" posted to its website, Hope College announced that on or around September 27, 2022, Hope College discovered "unauthorized access" to its network and engaged third-party specialists to conduct a forensic investigation.

21. Hope College's investigation determined that certain sensitive information kept in the normal course of business was subject to this "unauthorized access."

22. Hope College has stated the "information believed to be at risk includes individuals' first and last names, in combination with date of birth, Social Security number, driver's license number, and Student ID number."

23. Once Hope College discovered that certain files may have been accessed by an "unauthorized party," Hope College undertook a review process to identify what personal information was present. Hope College completed that review on November 8, 2022.

24. PII pertaining to Plaintiff, including his Social Security number, was part of the data acquired by the "unauthorized party" from Hope College's systems in the Data Breach.

25. Despite being aware of the Data Breach on September 27, 2022, Hope College failed to take any action to notify Plaintiff or other Class Members of this breach until at least December 15, 2022.

26. Hope College failed to take appropriate or even the most basic steps to protect the PII of Plaintiff and other Class Members from being disclosed.

27. In addition, Hope College consulted with its own "IT team" as well as "third party forensic and legal specialists" to assist its "investigation." Additional items of PII as well as other

facts surrounding the Data Breach may be uncovered or have already been uncovered and not yet publicly disclosed.

28. Hope College's Notice Letter and Notice of Data Security Event have notably omitted any change to its data security or retention policies. These are steps that should have been employed in the first place-and which would have prevented or limited the impact of the Data Breach.

29. As a result of the Data Breach, Plaintiff and Class Members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

B. Data Security Industry Standards

30. Defendant is well aware of the importance of safeguarding Plaintiff's and Class Members' PIII, that by virtue of its business—as a higher education institution—it places Plaintiff's and Class Members' PII at risk of being targeted by cybercriminals.

31. Defendant is aware that the PII that it collects, organizes, and stores, can be used by cybercriminals to engage in crimes such as identity fraud and theft using Plaintiff's and Class Members' PII.

32. Because Defendant failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, Defendant was unable to protect Plaintiff's and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

33. As a proximate result of such failures, cybercriminals gained unauthorized access to Defendant's network and acquired Plaintiff's and Class Members' PII in the Data Breach without being stopped.

34. Defendant was unable to prevent the Data Breach and was unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiff's and Class Members' PII.

35. Commonly accepted data security standards among businesses and higher education institutions that store personal information, such as the PII involved here, include, but are not limited to:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

36. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for Cybersecurity (*Start with Security: A Guide for Business*, (June 2015)) and protection of personal and financial information (*Protecting Personal Information: A Guide for Business* (Oct. 2016)), which includes basic security standards applicable to all types of businesses and higher education institutions.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses and higher education institutions must take to meet their data security obligations.

38. Because Defendant was entrusted with Plaintiff's and Class Members' PII, it had and has a duty to keep the PII secure.

39. Plaintiff and Class Members reasonably expect that when they entrusted their PII to Hope College it will safeguard their information.

40. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

41. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

C. Defendant Violated Its Common Law Duty of Reasonable Care

42. Defendant was aware of the importance of security in maintaining personal information (particularly sensitive personal information like the PII involved here), and the value consumers place on keeping their PII secure.

43. In addition to obligations imposed by federal and state law, Defendant owed and continues to owe a common law duty to Plaintiff and Class Members—who entrusted Defendant with their PII—to exercise reasonable care in receiving, maintaining, and storing, the PII in Defendant's possession.

44. Defendant owed and continues to owe a duty to prevent Plaintiff's and Class Members' PII from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendant's duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiff's and Class Members' PII.

45. Defendant owed a duty to Plaintiff and Class Members, who entrusted Defendant with extremely sensitive PII to design, maintain, and test the information technology systems that housed Plaintiff's and Class Members' PII, to ensure that the PII in Defendant's possession was adequately secured and protected.

46. Defendant owed a duty to Plaintiff and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the PII stored in Defendant's systems. In addition, this duty also required Hope College to adequately train its employees and others with access to Plaintiff's and Class Members' PII on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Hope College's part to ensure that it complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' PII.

47. Defendant owed a duty to Plaintiff and Class Members to implement processes that would enable Defendant to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

48. Defendant owed a duty to Plaintiff and Class Members to disclose when and if its information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiff's and Class Members' PII.

49. As the Notice of Data Security Event states, "[u]pon discovery" of the "unauthorized access," Hope College immediately "began working with its IT team, and third-party forensic and legal specialists were engaged to conduct a full forensic investigation." Hope College could have taken these steps *beforehand* to protect the PII in their possession and prevent the Data Breach from occurring, as required under the common law, FTC guidelines, as well as other state and federal law and/or regulations.

50. Thus, Defendant owed a duty to Plaintiff and Class Members to timely disclose the fact that a data breach, resulting in unauthorized access to their PII, had occurred.

51. Defendant violated these duties. The Notice Letter and Notice of Data Security Event further states that Hope College became aware of the Data Breach on September 27, 2022, however Plaintiff and Class Members, and the public did not learn of the Data Breach until December 15, 2022, when the Notice Letters were mailed out. Defendant failed to publicly describe the full extent of the Data Breach and notify affected parties. This demonstrates that Hope College did not properly implement measures designed to timely detect a data breach of their information technology systems, as required to adequately safeguard Plaintiff's and Class Members' PII.

52. Defendant also violated its duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' PII.

D. The Value of Private Information and Effects of Unauthorized Disclosure

53. Defendant was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

54. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

55. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

56. The forms of PII involved in this Data Breach are particularly concerning, including:

57. ***Social Security numbers***—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of

the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

58. Indeed, even the Social Security Administration warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

59. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain goods or services. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

60. ***Driver's license numbers***—are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive.

61. *Experian*, a globally recognized credit reporting agency, has explained "[n]ext to your Social Security number, your driver's license number is one of the most important pieces of

information to keep safe from thieves." This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV and other government agencies, places of employment, doctor's offices, and other entities.

62. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced.

63. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

64. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their accounts *ad infinitum*.

65. Thus, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

66. As a highly sophisticated party that handles sensitive PII, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' PII to protect against anticipated threats of intrusion of such information.

67. Identity thieves use stolen PII for various types of criminal activities, such as when personal information is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

68. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

69. There is often a lag time between when fraud occurs versus when it is discovered, as well as between when PII is stolen and when it is used. According to the *U.S. Government Accountability Office*, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

70. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

71. Plaintiff and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

72. Thus, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

73. Data breaches are preventable. As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…" and "[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures…Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

74. The types PII, such as Social Security and driver's license numbers, compromised in the Data Breach are immutable. Plaintiff and Class Members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of Plaintiff's and Class Members' information to commit serious identity theft and fraud.

E. Defendant Failed to Comply with the FTC Act

75. Defendant is prohibited by the Section 5 of the FTC Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has

concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

77. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

78. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

79. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

80. Defendant is aware of and failed to follow the FTC guidelines and failed to adequately secure PII.

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

82. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

83. Defendant was at all times fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and storing PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Plaintiff and Class Members Suffered Harm

84. The ramifications of Defendant's failure to keep PII secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

85. Plaintiff and Class Members have faced a substantial and imminent risk of identity theft and fraud as a result of the Data Breach. Unauthorized third parties carried out the Data Breach and stole the personal information of Plaintiff and Class Members with the intent to use it for fraudulent purposes and/or sell it to other cybercriminals.

86. The risk of identity theft is particularly substantial when the PII compromised is unique to a specific individual, as it is here, and is extremely sensitive Social Security and driver's license numbers.

87. Plaintiff and Class Members will spend substantial amounts of their money and time monitoring their accounts for identity theft and fraud and reviewing their affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming.

88. Plaintiff and Class Members now face years of constant surveillance of their personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

89. Besides damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

90. Despite all of the publicly available knowledge of the continued compromises of PII and the importance of securing such information, Defendant's commitment to secure its customers' information fell by the wayside.

91. Hope College was well aware of the requirements and obligations to secure PII. Further, Hope College had control over the configuration and design of its own systems, and knowingly chose to forego the necessary data protection techniques needed for it to secure Plaintiff's and Class Members' PII.

92. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impeding injury flowing from fraud and identity

theft posed by their PII being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their PII; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

CLASS ACTION ALLEGATIONS

93. Plaintiff brings this case individually and, pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following Nationwide Class and Michigan Subclass (collectively the "Class"):

> **Nationwide Class**
> All persons whose PII was compromised in the Data Breach that was discovered by Hope College on or around September 27, 2022.
>
> **Michigan Subclass**
> All residents of Michigan whose PII was compromised in the Data breach that was discovered by Hope College on or around September 27, 2022.

94. Excluded from the Class are Defendant, its subsidiaries and affiliates, its officers, directors and members of its immediate families and any entity in which Defendant have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

95. Plaintiff reserves the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

96. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will

benefit both the parties and this Court. As noted above, there are approximately 156,783 Class Members.

97. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

98. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to secure and protect the PII of Plaintiff and Class Members;

b. Whether Defendant were negligent in collecting and disclosing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

j. Whether Plaintiff and Class Members are entitled to declaratory judgment under 28 U.S.C. § 2201, *et seq.*;

k. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

99. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiff and Class Members each had their PII disclosed by Defendant to an unauthorized third party.

100. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation, including data breach litigation. The claims of Plaintiff and Class Members are substantially

identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

101. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

102. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

103. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION
COUNT I
NEGLIGENCE

104. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

105. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

106. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected; (b) implementing processes that

would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; (d) maintaining data security measures consistent with industry and governmental regulator standards.

107. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

108. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

109. Defendant had a duty not to engage in conduct that creates a foreseeable risk of harm to Plaintiff and Class Members.

110. Defendant breached the duties owed to Plaintiff and Class Members and thus were negligent. Specifically, Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry and governmental regulator standards; and (d) disclose that Plaintiff's and Class Members' PII in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

111. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

112. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

(a) Theft of their PII;

(b) Costs associated with requested credit freezes;

(c) Costs associated with the detection and prevention of identity theft;

(d) Costs associated with purchasing credit monitoring and identity theft protection services;

(e) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of Defendant's Data Breach;

(f) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being disclosed to cybercriminals;

(g) Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the societal understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

(h) Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

113. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

COUNT II
NEGLIGENCE *PER SE*

115. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

116. Hope College's duties arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1).

117. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

118. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

119. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

120. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

121. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

122. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

123. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

COUNT III
BREACH OF FIDUCIARY DUTY

124. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

125. Plaintiff and Class Members either directly or indirectly gave Hope College their PII in confidence, believing that Hope College – a higher education institution – would protect that information. Plaintiff and Class Members would not have provided Hope College with this information had they known it would not be adequately protected. Hope College's acceptance and storage of Plaintiff's and Class Members' PII created a fiduciary relationship between Hope College and Plaintiff and Class Members. In light of this relationship, Hope College must act primarily for the benefit of its customers and students, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

126. Hope College has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTC Act, and otherwise failing to safeguard the PII of Plaintiff and Class Members it collected.

127. As a direct and proximate result of Hope College's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i)

a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Hope College's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

128. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

129. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

COUNT IV
UNJUST ENRICHMENT

130. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

131. Plaintiff and Class Members conferred a monetary benefit upon Hope College in the form of monies paid for educational services and/or other services.

132. Hope College accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Hope College also benefitted from the receipt of Plaintiff's and Class Members' PII.

133. As a result of Hope College's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

134. Hope College should not be permitted to retain the money belonging to Plaintiff and Class Members because Hope College failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

135. Hope College should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT

136. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

137. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for Hope College to provide services. In exchange, Hope College entered into implied contracts with Plaintiff and Class Members in which Hope College agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

138. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

139. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

140. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and adequate notice of the Data Breach.

141. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

142. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

143. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

COUNT VI
VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT
(Mich. Comp. Laws Ann § 445.901, *et. seq.*)

144. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

145. The Michigan Consumer Protection Act was created to protect Michigan consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

146. Plaintiff and Class members provided PII to Defendant pursuant to transactions (i.e., providing education) they engaged in with Defendant as customers and students.

147. Defendant has its principal place of business and headquarters in Michigan and transacts with Michigan consumers and students.

148. Hope College engaged in deceptive trade practices in the conduct of its business, in violation of Mich. Comp. Laws Ann § 445.901, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

149. Hope College's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify Plaintiff, and class members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' PII; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

150. 109. Hope College's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Hope College's data security and ability to protect the confidentiality of consumers' PII.

151. Hope College's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Class Members, that their PII was not exposed and misled Plaintiff and the Class Members into believing they did not need to take actions to secure their identities.

152. Hope College intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

153. Had Hope College disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Hope College would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Hope College was trusted with sensitive and valuable PII regarding hundreds of thousands of consumers, including Plaintiff and Class Members. Hope College accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Hope College held itself out as maintaining a secure platform for PII data, Plaintiff and the Class Members acted reasonably in relying on Hope College's misrepresentations and omissions, the truth of which they could not have discovered.

154. As a direct and proximate result of Hope College's deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

155. Class Members are likely to be damaged by Hope College's ongoing deceptive trade practices.

156. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

157. Accordingly, pursuant to Mich. Comp. Law Ann. § 445.901, *et seq.*, Plaintiff and Class Members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages

are: (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud; and other miscellaneous incidental and consequential damages.

158. In addition, given the nature of Hope College's conduct, Plaintiff and Class Members are entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from Hope College's unlawful conduct.

COUNT VII
DECLARATORY JUDGMENT

159. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

160. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

161. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

162. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure consumers' PII and to timely and adequately notify consumers of a data breach under the common law, Section 5 of the FTC Act, and the Michigan Consumer Protection Act, Mich. Comp. Laws Ann § 445.901, *et seq.*;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' PII; and

c. Defendant's ongoing breaches of its legal duty continues to cause Plaintiff harm.

163. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect Plaintiff's and Class Members' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

164. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not

have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

165. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

166. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and all others similarly situated, prays for relief as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For damages, including all compensatory, punitive, and/or nominal damages, in an amount to be determined by the trier of fact;

(d) For an order of restitution and all other forms of equitable monetary relief;

(e) Declaratory and injunctive relief as described herein;

(f) Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

(g) Awarding pre- and post-judgment interest on any amounts awarded; and

(h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: January 30, 2023

Respectfully submitted

THE MILLER LAW FIRM, P.C.

/s/ E. Powell Miller
E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
Emily E. Hughes (P68724)
950 W. University Dr., Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
ssa@millerlawpc.com
eeh@millerlawpc.com

SHUB LAW FIRM LLC
Jonathan Shub*
Benjamin F. Johns*
Samantha E. Holbrook*
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

LOWEY DANNENBERG, P.C.
Christian Levis*
Amanda G. Fiorilla*
44 South Broadway, Suite 1100
White Plains, NY 10601
T: (914) 997-0500
clevis@lowey.com
afiorilla@lowey.com

LOWEY DANNENBERG, P.C.
Anthony M. Christina*
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
T: (215) 399-4770
achristina@lowey.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice Forthcoming*